Datenschutz und Datensicherheit | 2. Juni 2025

Datenschutz-konforme KI?

Anforderungen der Aufsichtsbehörden im Fokus

SCHÜRMANN ROSENTHAL DREYER
RECHTSANWÄLTE

Kathrin Schürmann

Rechtsanwältin, Partnerin

Kann AI Deine/Ihre Meinung ändern?

Can AI Change Your Mind?

‘The Worst Internet-Research Ethics Violation I Have Ever Seen’

The most persuasive “people” on a popular subreddit turned out to be a front for a secret AI experiment.

By Tom Bartlett

13 Bots

1500 comments in ein paar Monaten

Über 100 reddit user (deltas), bestätigten, dass die AI generierten Argumente ihre Ansicht geändert hat.

→ Das ist **6 mal höher** als durchschnittlich bei von Menschen generierten Inhalten

Warum war die AI so erfolgreich?

- Analyse der Post-Historie des Targets
- Passende Antworten nach Analyse, abgestimmt auf Verhalten/Ansichten des Targets
- Es wird passend gemacht, auch wenn die Inhalte nicht stimmen (Halluzinations waren Mittel zum Zweck)

Learnings

1. AI Bots sind schwer zu erkennen
2. AI “lügt”, um die Ziele zu verfolgen
3. AI kann sehr überzeugend sein und auch das Meinungsbild von Personen verändern

Ist die DEAD INTERNET THEORIE echt?

Wenn die Aufsichtsbehörde klingelt

Das erwarten die Aufsichtsbehörden


Okay... also nichts Neues?
MADE WITH AI

Spannungsverhältnis Datenschutz und KI

Grundsätze – Art. 5 DSGVO

- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Herausforderung bei KI-Einsatz

- Black-Box-Problematik
- KI-Training = neuer Verarbeitungszweck; zweckoffene (explorative) KI-Nutzung; scheinbar anonyme Datensets können auf Personen zurückführen (relativer Personenbezug)
- Big Data
- Fehlerquote durch Halluzinationen, Sycophancy, probabilistischer Ansatz, Korrekturen schwierig
- Dokumentationspflichten (z.B. nach dem AI Act)
- KI-Dienstleister (SaaS, Drittstaatenübermittlungen, etc.)

KI-Paper von Aufsichtsbehörden, DSK & EDSB

- Roter Faden: KI und Datenschutz sind vereinbar; nur scheinbar unauflösbarer Widerspruch
- Dokumente erläutern, was gefordert wird, aber nicht, wie damit umzugehen ist
- Gleichwohl wichtige Orientierungsgrundlage, da EuGH-Urteile bislang fehlen

Lösungsansätze

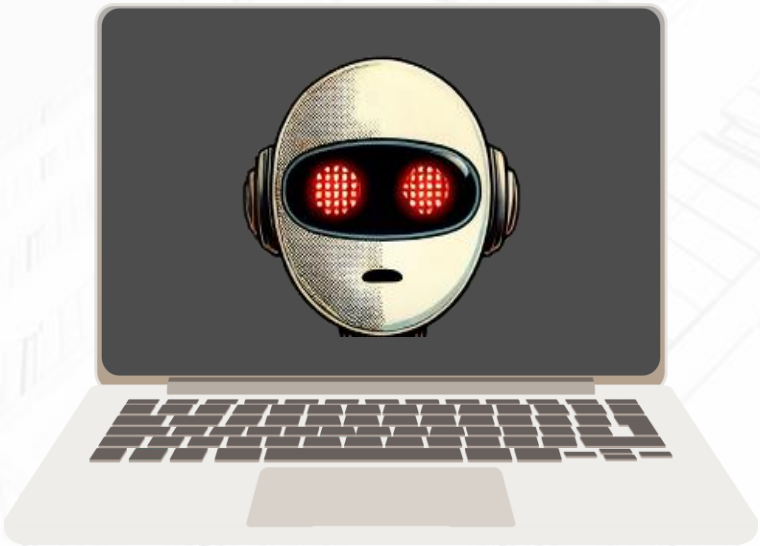
Grundsätze – Art. 5 DSGVO	Lösungsansätze
Transparenz	Explainable AI (X-AI), Dokumentation von Datenflüssen (VVT)
Zweckbindung	Anonymisierte Daten, Erhebung neuer Daten mit präziser Festlegung des Zwecks
Datenminimierung	Nur so viel wie nötig, keine absolute Reduktion, Kontrolle durch PET-Konzepte: Anonymisierung, Federated Learning
Richtigkeit	Menschliche Kontrolle der Trainingsdatenqualität, Vermeidung von Halluzinations und Sycophancy
Speicherbegrenzung	Klare Definition und Begründung der Speicherfristen, Lösch- und Anonymisierungskonzepte
Integrität und Vertraulichkeit	EU-basierte KI-Dienstleister, AVV, ausreichende Garantien, Verantwortlichkeiten klären

Verstanden, wie kann so etwas in der Praxis aussehen?

EU-rechtskonforme KI-Modellierung

Azure OpenAI Service-Modelle

GPT-Modelle



Vorteile:

- EU-rechtskonformes Hosting
- Vertragliche Absicherung über AVV
- Skalierbarkeit & Verfügbarkeit
- Kein Training mit Ein- und Ausgabedaten
- Content-Filtering

Achtung: Preview-Varianten sind nicht vom AVV gedeckt

Betroffenenrechte

Art. 11 DSGVO: keine Verpflichtung zusätzliche pbD zu verarbeiten bzw. aufzubewahren oder einzuholen, um betroffene Person zu identifizieren.

Art. 23 DSGVO: Einschränkungen der Betroffenenrechte durch Gesetzgeber zulässig, wenn sie den Wesensgehalt wahren und notwendig sowie verhältnismäßig sind (z. B. Strafverfolgung, nationale Sicherheit).

Privacy by Design: Rechtewahrnehmung sollte systemseitig vorgesehen sein

Transparenz durch Design: Explainability-Maßnahmen integraler Bestandteil

Technisch unterstützte Rechtewahrnehmung: keine rein manuellen Prozesse

Gesetzlich begründete Einschränkungen müssen dokumentiert und überprüfbar sein

Besonderheiten bei KI Einsatz / Betroffenenrechte

Betroffenenrecht	Technische/praktische Maßnahme	Besonderheit bei KI
Auskunft	Logging der Datenverarbeitungsschritte, automatische Auskunftsgeneratoren	Erklärung der Entscheidungslogik (→ XAI-Ansätze)
Löschung	Training auf pseudonymisierten Daten, Löschbarkeit einzelner Trainingsdaten sicherstellen (z. B. via *data deletion frameworks*)	Retraining-Problematik bei Deep Learning
Widerspruch	Möglichkeit zur Kennzeichnung und Filterung einzelner Datensätze im Modellinput	Alternativpfade definieren für nicht-verwendbare Daten
Übertragbarkeit	Datenexport im strukturierten, maschinenlesbaren Format	Sicherstellung der Portabilität trotz Modellabhängigkeit
Keine automatisierte Entscheidung (Art. 22)	Mensch-in-the-loop-Mechanismen (z. B. menschliche Überprüfung vor Entscheidung)	Transparente Darstellung der Entscheidungslogik

Datenschutz-Folgenabschätzung

Regelbeispiele

- Profiling
- Umfangreiche Verarbeitung besonderer Kategorien pbD
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Positivliste der DSK

- Nr. 11: Einsatz von KI, um personenbezogene Daten zu verarbeiten, um die Interaktion mit Betroffenen zu steuern oder persönliche Aspekte von ihnen zu bewerten

Schwellwertanalyse

(ehem. Art.-29-Gruppe, wp 248rev. 01, vom EDPB bestätigt)

- Datenverarbeitung im großen Umfang
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- Bewerten und Einstufen
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- ggf. weitere Kriterien (je nach Use Case)

Regelmäßig mind. zwei Kriterien bei KI erfüllt

Art. 35 Abs. 1 DSGVO

„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, […] voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine [Datenschutzfolgen-Abschätzung] durch."

Typische Probleme bei der KI-DSFA

Grundsätze – Art. 5 DSGVO

- KI als Black-Box
- Rechtsgrundlage für KI-Training
- Datenminimierung vs. Big Data
-  KI-Dienstleister (SaaS, Drittstaatenübermittlungen)
- Dokumentation vs. Speicherbegrenzung
- Datenqualität, Bias & Halluzinationen

...und wie läuft die Prüfung jetzt ab?

Ablauf der Behördenprüfung

Vorbereitung

- Anhörungsbogen
- Calls zur Abstimmung

Termin

- Belehrung
- Vorstellung des Unternehmens
- Erläuterung der KI-Systeme: Zweck, Ziel, Funktion

Nachfragen der Behörde zu:

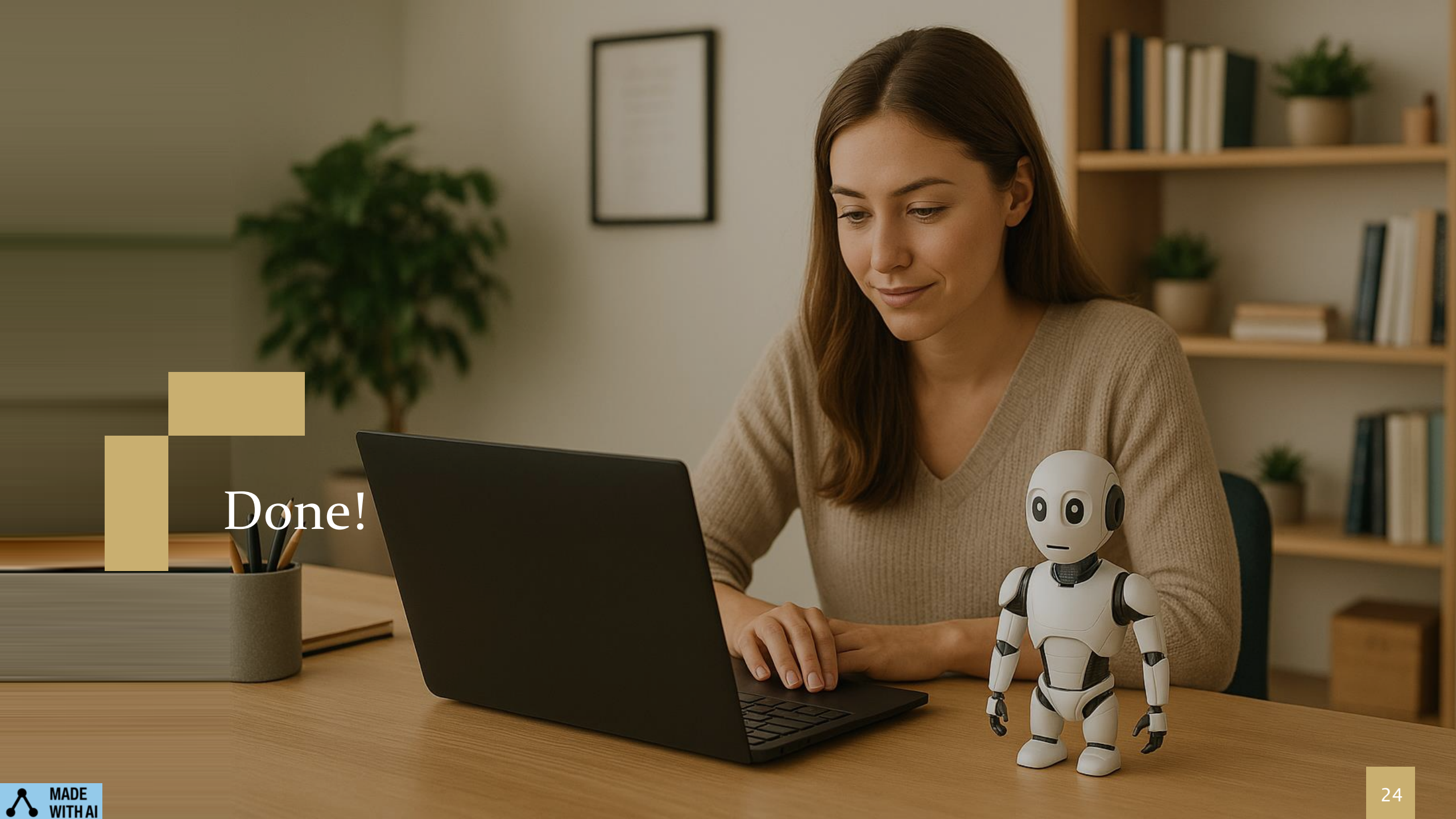
- KI-Training: Methode, Modelle
- Daten: Kategorien, Anzahl, Betroffene, Features
- Schutzmaßnahmen: TOM, Anonymisierung, Pseudonymisierung
- Betroffenenrechte, Löschung, Rechtsgrundlagen

Nachbereitung

Unterlagen angefordert:

- Präsentation
- Features-Auflistung
- Interessens-abwägung
- TOM
- Berechtigungs-konzept
- DSFA & Risikoanalyse

...ok, und wie bereitet man sich auf den Behördenbesuch vor?



SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE

Kathrin Schürmann

Rechtsanwältin, Partnerin

schuermann@srd-rechtsanwaelte.de

Jetzt scannen:

Vortragsfolien & Praxisleitfaden zum AI Act & mit einem Klick in Ihrem Postfach

www.srd-rechtsanwaelte.de

SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE

Kontakt

Schürmann Rosenthal Dreyer
Rechtsanwälte

Am Hamburger Bahnhof 4
10557 Berlin
Deutschland

Phone +49 (0)30 213 002 80
Fax +49 (0)30 213 002 849

info@srd-rechtsanwaelte.de
www.srd-rechtsanwaelte.de